Information technology-Security techniques-Information security management systems-Requirements

信息技术
安全技术
信息安全管理体系要求

版本历史

版本	作者	日期	变更内容	备注
1.0	刘青	2005.11	初始版本翻译	
1.1	李鹏飞	2005.11	校对，添加附录	

文件说明

本文档初始版本为刘青(高级咨询顾问、BS7799LA)翻译,在此特别感谢刘青。本人学习之后对其中的点滴做了校正，以方便同行更好的学习。因本人水平有限，其中难免有不妥之处，如果有疑问可以联系刘青和我。

刘青联系方式：

邮箱：liuq@koal.com
MSN：liuq1217@msn.com
电话：010-65541200-163
传真：010-65542918
手机：138 1116 0364

我的联系方式：

邮箱：lipengfei@tass.com.cn
MSN：pengfeilee@hotmail.com
电话：010-82326383-8046
传真：010-82328039
手机：137 1763 0843

再次感谢刘青所做的工作。

李鹏飞

2005 年 11 月

前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了全世界标准化的专门体系。作为ISO 或IEC 成员的国家机构，通过相应组织所建立的涉及技术活动特定领域的委员会参加国际标准的制定。ISO 和IEC 技术委员会在共同关心的领域里合作，其它与ISO 和IEC 有联系的政府和非政府的国际组织也参加了该项工作。在信息安全领域，ISO 和IEC 已经建立了一个联合技术委员会－ISO/IEC JTC 1。

国际标准的起草符合ISO/IEC 导则第2 部分的原则。

联合技术委员会的主要任务是起草国际标准。联合技术委员会采纳的国际标准草案分发给国家机构投票表决。作为国际标准公开发表，需要至少75%的国家机构投赞成票。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意，ISO 不负责标识任何这样的专利权问题。

国际标准ISO/IEC 27001 是由联合技术委员会ISO/IEC JTC1（信息技术）的SC27 分会（安全技术）起草的。

目 录

0 简介

0.1 总则

本标准为建立、实施、运作、监视、评审、保持和改进信息安全管理体系（ISMS）提供了模型。ISMS的采用是组织的战略性决策。组织ISMS的设计和实施受组织需求、目标、安全需求、应用的过程以及组织规模和结构的影响。经过一段时间，组织及其支持系统会发生改变。因此ISMS的实施应与组织的需要相一致，如，简单的环境只需要一个简单的ISMS解决方案。

本标准可被内部、外部的相关方用于评估符合性。

0.2 过程方法

本标准鼓励在建立、实施、运作、监视、评审、保持和改进组织的ISMS时采用过程方法。

为使组织有效运作，必须识别和管理众多相互关联的活动。通过利用资源和管理，将输入转化为输出的一项活动，可以视为一个过程。通常，一个过程的输出可直接形成下一过程的输入。

组织内过程系统的应用，连同这些过程的识别和相互作用及其管理，可称之为“过程方法”。

本标准所引用的信息安全管理过程方法在应用时强调以下方面的重要性：

a) 了解组织的信息安全要求及建立信息安全策略和目标的需求；

b) 在组织的整体业务风险框架内，通过实施和运行控制以管理组织的信息安全风险；

c) 监视和评审ISMS的执行和有效性；

d) 基于客观测量的持续改进。

本标准采用PDCA“规划-执行-控制-改进”（PDCA）过程模式。该模型适用于建立ISMS的所有过程。图1描述了ISMS如何输入相关方的信息安全要求和期望，经过必需的活动和过程，产生满足这些需求和期望的信息安全输出。图1也展示

了4、5、6、7和8章中所引用过程的联系。

采用PDCA模型也反应了OECD指南（2002）《信息系统和网络的安全治理》中所陈述的准则。本标准为在风险评估、安全设计和实施、安全管理和再评估方面实施这些指南中的准则提供了强健模型。

例1 ：

要求可以是违背信息安全不会给组织带来严重经济损失或干扰。

例2：

期望可以是如果发生严重的安全事故(例如组织的商务网站被黑客攻击。)，有经过充分培训的人按适当的程序使影响最小化。

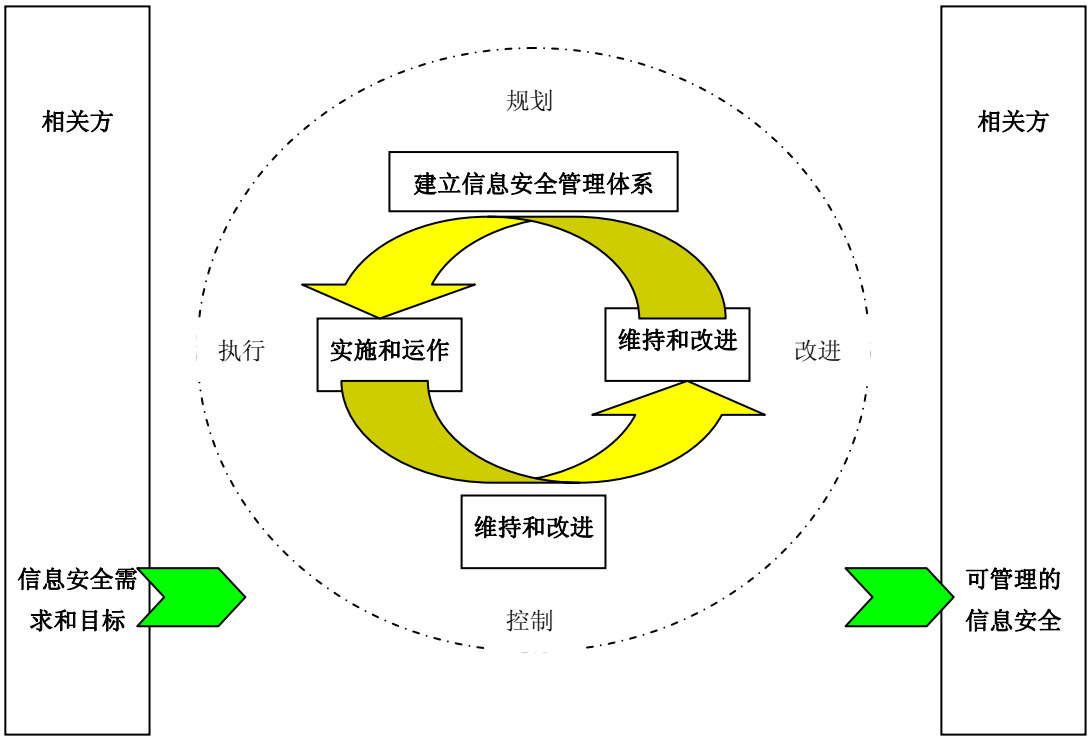

图-1 信息安全体系过程模型

规划（建立 ISMS）	根据组织的整体策略和目标，建立安全策略、目标以及与管理风险和改进信息安全相关的过程和程序，以获得结果。
执行（实施和运作 ISMS）	实施和运作安全策略、控制、过程和程序。
控制（监视和评审 ISMS）	适用时，根据ISMS策略、目标和惯有经验评估和测量过程的执行，并向管理层报告结果，进行评审。
改进（保持和改进 ISMS）	根据内部ISMS 审计和管理评审或其他信息，采取纠正和预防措施，以实现ISMS 的持续改进。

0.3 与其他管理体系的兼容性

本标准与ISO9001:2000和ISO14001:2004协调一致，以支持与相关管理标准的结合和整合的实施和运行。表C.1注了本标准与ISO9001:2000和ISO14001:2004的章节间的对应关系 。

本标准的设计使组织能将ISMS与相关管理体系相整合。

1 范围

1.1 总则

本标准覆盖了所有类型的组织（如商业企业、政府机构和非盈利组织）。本标准为根据组织整体业务风险建立、实施、运作、监视、评审、保持和改进文件化的信息安全管理体系规定了要求；为实施满足组织或组织部分的需求的安全控制规定了要求。

ISMS的设计提供了充分、适当的安全控制，充分保护信息资产，使相关方充满信心。

注1：标准中提及的“业务”是指对于组织存在的目的非常关键的活动。

注2：ISO/IEC 17799 为设计控制提供了实施指南。

1.2 应用

本标准所规定的要求是通用的，旨在适用于各种类型、不同规模和业务性质的组织。组织若对第4、5、6、7 和8 章的内容进行了任何删减，则不得宣称符合本标准。

需证明任何控制的删减满足风险接受的准则。应提供证据证明相关风险已被大多数人适当接受。除非删减不影响组织满足风险评估和适用法律要求的信息安全的能力和责任，否则不能声称符合本标准。

注：如果组织已经存在一个操作性业务过程管理体系（如ISO90001 或ISO14001），组织将在现有管理体系的范围内更好的满足本标准的要求。

2 引用标准

下列标准引用的条文在本标准中同样引用。对标注日期的条文只有引用的版本适用，未标注日期的条文最新版本适用。

ISO/IEC 17799：2005 信息技术－安全技术－信息安全管理实施指南

3 术语和定义

3.1 资产

任何对组织有价值的事物。

[ISO/IEC13335-1:2004]

3.2 可用性

需要时，授权实体可以访问和使用的特性。

[ISO/IEC13335-1:2004]

3.3 保密性

信息不可用或不被泄漏给未授权的个人、实体和过程的特性。

[ISO/IEC13335-1:2004]

3.4 信息安全

保护信息的保密性、完整性、可用性及其他属性，如：真实性、可核查性、可靠性、防抵赖性。

[ISO/IEC17799:2005]

3.5 信息安全事件（Event）

信息安全事件是指识别出的发生的系统、服务或网络事件表明可能违反信息安全策略或防护措施失效；或以前未知的与安全相关的情况。

[ISO/IEC TR 18044]

3.6 信息安全事故（Incident）

信息安全事故是指一个或系列非期望的或非预期的信息安全事件，这些信息安全事件可能对业务运营造成严重影响或威胁信息安全。

[ISO/IEC TR 18044]

3.7 信息安全管理体系（ISMS）

整体管理体系的一部分，基于业务风险方法以建立、实施、运行、监视、评审、保持和改进信息安全。

注：管理体系包括组织机构、策略、策划、活动、职责、惯例、程序、过程和资源。

3.8 完整性

保护资产的正确和完整的特性

[ISO/IEC13335-1:2004]

3.9 残余风险

实施风险处置后仍旧残留的风险。

[ISO/IEC Guide 73:2002]

3.10 风险接受

接受风险的决策。

[ISO/IEC Guide 73:2002]

3.11 风险分析

系统地使用信息以识别来源和估计风险。

[ISO Guide 73：2002]

3.12 风险评估

风险分析和风险评价的全过程

[ISO Guide 73：2002]

3.13 风险评价

将估计的风险与既定的风险准则进行比较以确定重要风险的过程。

[ISO Guide 73：2002]

3.14 风险管理

指导和控制一个组织的风险的协调的活动。

[ISO Guide 73：2002]

注：典型风险管理包括风险评估、风险处置、风险接受和风险沟通。

3.15 风险处置

选择和实施措施以改变风险的过程。

[ISO Guide 73：2002]

注：本标准中的术语“控制措施”等同于“措施”。

3.16 适用性声明

与组织ISMS 相关并适用于组织ISMS 的控制目标和控制措施的文件化的陈述。

注：控制目标和控制措施是基于风险评估和风险处置过程的结果和结论、法律法规要求、合同业务和组织对信息安全的业务要求。

4 信息安全管理体系

4.1 总要求

组织应根据整体业务活动及其面临的风险，建立、实施、运作、监视、评审、保持并改进文件化的信息安全管理体系。本标准应用了图1所示的PDCA模式。

4.2 建立并管理 ISMS

4.2.1 建立 ISMS

组织应：

a) 根据组织业务特征、组织、地理位置、资产、技术以及任何删减的细节和合理性来确定ISMS范围；

b) 根据组织业务特征、组织、地理位置、资产和技术确定ISMS策略，策略应：

1). 包括建立目标的框架，并建立信息安全活动的总方向和总原则；

2). 考虑业务和法律法规要求，以及合同安全义务；

3). 根据组织战略性的风险管理，建立和保持ISMS；

4). 建立风险评价的准则和定义风险评估的结构 [见4.2.1c]；

5). 经过了管理层的批准。

注：本文件中将ISMS策略作为信息安全策略的一个扩展集。这些策略可以在同一个文件中描述。

c) 定义组织的风险评估方法

1). 识别适用于ISMS、已识别的业务信息安全和法律法规要求的风险评估方法；

2). 开发确定风险接受准则，识别风险的可接受等级[见5.1f]。

风险评估方法的选择应确保可以产生可比较的、可重复的结果。

注：存在多种风险评估方法。如，在ISO/IEC TR13335-3《IT安全管理指南－IT安全管理技术》中讨论的风险评估方法

d) 识别风险：

1). 识别ISMS范围内的资产及资产所有者；

2). 识别资产的威胁；

3). 识别可能被威胁利用的脆弱点；

4). 识别资产保密性、完整性、可用性损失的影响。

e) 分析并评估风险：

1). 评估安全失效可能导致的组织业务影响，考虑因资产保密性、完整性、可用性的损失而导致的后果；

2). 根据资产的主要威胁、脆弱性、有关的影响以及已经实施的安全控制，评估安全失效发生的现实可能性；

3). 评估风险的等级 ；

4). 根据4.2.1c）2）已建立的风险接受准则，判断风险是否可接受或需要处置。

f) 识别和评价风险处置的选项：

可行的措施包括：

1). 实施适当的控制；

2). 在确切满足组织策略和风险接受准则的前提下，有意识地、客观地接受风险[见4.2.1c）2）] ；

3). 回避风险；

4). 将相关业务风险转嫁给他方，如保险公司、供方。

g) 选择风险处置的控制目标和控制方式。

应选择控制目标和控制措施，以满足风险评估和风险处置过程所识别的要求。选择时，应考虑接受风险的准则（见4.2.1 C））以及法律法规和合同要求。

从附录A中选择的控制目标和控制方式应作为这一过程的一部分，并满足这些要求。

附录A的控制目标和控制方式并不详尽，可以选择其他的控制目标和控制方式。

注：附录A包含了广泛的通用控制目标和控制措施列表。本标准的附录A为用户提供选择控制措施的出发点，以避免遗漏重要的控制选择。

h) 管理层批准建议的残留风险；

i) 获得管理层对实施和运作ISMS的授权；

j) 准备适用性声明

应起草适用性声明，该声明应包括以下方面内容：

1) 4.2.1g)中选择的控制目标和控制措施，以及选择的原因；

2) 最新实施的控制目标和控制措施（见4.2.2e）2)）

3) 附录A中控制目标和控制措施的删减，以及删减的合理性。

注：适用性声明提供了一个风险处置决策的总结。通过判断删减的合理性，再次确认控制目标没有被无意识的遗漏。

4.2.2 实施和运作 ISMS

组织应:

a) 阐明风险处置计划，它为信息安全风险管理（见第5章）指出了适当的管理措施、资源、职责和优先级；

b) 实施风险处置计划以达到确定的控制目标，应考虑资金需求以及角色和职责分配；

c) 实施4.2.1g）选择的控制措施以达到控制目标；

d) 确定如何测量所选择的一组控制措施的有效性，并规定这些测量措施如何用于评估控制的有效性以得出可比较的、可重复的结果；

注：测量控制措施的有效性允许管理者和相关人员来确定这些控制措施实现策划的控制目标的程度。

e) 实施培训和意识方案（见5.2.2）；

f) 管理ISMS的运作；

g) 管理ISMS资源（见5.2）；

h) 实施程序及其它控制以及时检测、响应安全事故（见4.2.3）。

4.2.3 监视和评审 ISMS

组织应：

a) 执行监视和评审程序和其它控制措施：

1). 及时检测过程结果中的错误；

2). 及时识别失败的或成功的安全违规和事故；

3). 使管理层能确定是否将安全活动授权，或由信息技术实施的安全活动是否按期望的实施；

4). 帮助检测安全事件，进而使用指标预防安全事故；

5). 确定所采取的措施是否有效解决安全违规。

b) 定期评审ISMS的有效性（包括安全策略和目标的实现情况，安全控制评审），考虑安全审核、事故、有效性测量的结果以及所有相关方的建议和反馈；

c) 测量控制措施的有效性，以证实安全要求已得到满足；

d) 按照计划的时间间隔，评审风险评估，并评审残余风险的等级和已识别的接受风险，考虑以下方面的变化：

1). 组织；

2). 技术；

3). 业务目标和过程；

4). 已识别的威胁；

5). 已实施的控制措施的有效性；

6). 外部事件，如法律法规、合同要求和社会风气的变化。

e) 按计划的时间间隔进行ISMS内部审核（见第6条款）；

注：内部审核，也称为第三方审核，是为了内部的目的，由组织或以组织的名义进行的审核。

f) 定期进行ISMS管理评审（至少一年一次），确保范围仍然充分，并识别ISMS过程改进的机会（见7.1）；

g) 更新安全计划，考虑监视和评审活动的发现；

h) 记录可能影响ISMS有效性或执行的措施和事件（见4.3.3）

4.2.4 保持和改进 ISMS

组织应定期进行：

a) 实施ISMS已识别的改进；

b) 按照8.2和8.3的要求采取适当的纠正和预防措施。总结从其它组织或组

织自身的安全经验得到的教训；

c) 与所有相关方沟通措施和改进。沟通的详细程度应与环境相适宜，必要是，应约定如何进行；

d) 确保改进活动达到了预期的目的。

4.3 文件要求

4.3.1 总则

文件应包括管理决策的记录，以确保措施可以追溯到管理决策和策略，记录的结果是可复制的。

重要的是要能够展示从选择的控制措施回溯到风险评估和风险处置过程结果的关系，最终回溯到ISMS 策略和目标。

ISMS 文件应包括：

a) ISMS策略（见4.2.1b））和控制目标的陈述；

b) ISMS 范围（见4.2.1a））；

c) ISMS 的支持性程序和控制；

d) 风险评估方法的描述（见4.2.1a））；

e) 风险评估报告（见4.2.1c）到4.2.1g））；

f) 风险处置计划（见4.2.2b））；

g) 组织为确保其信息安全过程的有效规划、运作和控制以及规定如何测量控制措施有效性所需的程序文件（见4.2.3 c））；

h) 本标准所要求的记录（见4.3.3）。

i) 适用性声明。

注1：本标准出现“文件化的程序”之处，即要求建立该程序，形成文件，并加以实施和保持。

注2：不同组织的ISMS文件的详略程度不同，取决于：

--组织的规模和活动的类型；

--被管理的系统和安全要求的范围和复杂程度。

注3：文件和记录可采用任何形式的媒体。

4.3.2 文件控制

ISMS所要求的文件应予以保护和控制。应编制形成文件控制程序，以规定以下方面所需的管理措施：

a) 文件发布前得到批准，以确保文件是充分的；

b) 必要时，对文件进行评审与更新并再次批准；

c) 确保文件的更改和现行修订状态得到标识；

d) 确保在使用处可获得适用文件的相关（最新）版本；

e) 确保文件保持合法，易于标识；

f) 确保文件可以为需要者所获得，并根据适用于他们类别的程序进行转移、存储和最终的销毁；

g) 确保外来文件得到标识；

h) 确保文件的分发是受控的；

i) 防止作废文件的非预期使用；

j) 若因任何原因而保留作废文件时，对这些文件进行适当的标识。

4.3.3 记录控制

应建立并保持记录，以提供符合要求和ISMS有效运作的证据。应保护并控制记录。ISMS应考虑相关的法律要求和合同责任。记录应保持合法，易于识别和检索。应编制形成文件的程序，以规定记录的标识、储存、保护、检索、保存期限和处置所需的控制。

保持4.2列出的过程执行的记录以及与ISMS有关的重大安全事件的记录

举例：

记录包括访问者登记表、审核记录和完成的访问授权表。

5 管理职责

5.1 管理承诺

管理层应通过以下措施对其建立、实施、运作、监视、评审、保持和改进ISMS的承诺提供证据：

a) 建立ISMS策略；

b) 确保ISMS目标和计划的建立；

c) 为信息安全分配角色和职责；

d) 向组织传达实现信息安全目标、符合信息安全策略、法律责任的重要性以及持续改进的需要；

e) 提供足够的资源，以建立、实施、运作、监视、保持和改进ISMS（见5.2.1）；

f) 决定接受风险准则和风险的可接受等级；

g) 确保ISMS内部审计的实施（见第6章）

h) 进行ISMS管理评审（见第7章）。

5.2 资源管理

5.2.1 资源提供

组织应确定并提供以下方面所需的资源：

a) 建立、实施、运作、监视、评审、保持和改进ISMS；

b) 确保信息安全程序支持业务需求；

c) 识别并指出法律法规要求和合同安全责任；

d) 通过正确应用实施的所有控制来保持足够的安全；

e) 需要时进行评审，并对评审的结果采取适当措施；

f) 必要时，改进ISMS的有效性。

5.2.2 培训，意识和能力

组织应确保在ISMS中承担责任的人员应能够胜任要求的任务：

a) 确定从事影响ISMS工作人员所必需的能力；

b) 提供培训或采取其他的措施（如雇佣有能力的人员）来满足这些需求；

c) 评估所提供培训和所采取措施的有效性；

d) 保持教育、培训、技能、经验和资质的记录（见4.3.3）。

组织应确保所有相关人员认识到，他们的信息安全活动的相关性和重要性，以及他们如何为实现ISMS目标做出贡献。

6 ISMS 内部审计

组织应按有计划的时间间隔进行ISMS内部审计，以确定组织ISMS的控制目标、控制措施、过程和程序是否：

a) 符合本标准及相关法律法规的要求；

b) 符合已识别的信息安全要求；

c) 得到有效地实施和保持；

d) 按期望执行。

应策划审计方案，考虑审计过程和区域的状况及重要性，以及上次审计的结果。定义审计的准则、范围、频次和方法。审计员的选择和审计的实施应保证设计过程的客观和公正。审计员不能审计自己的工作。

应定义文件化的程序，以规定策划和指导审计、报告结果和保持记录（见4.3.3）的职责和要求。

受审计区域的负责人应确保立即采取措施以消除发现的不符及其原因。跟踪活动应包括所采取措施的验证以及验证结果的报告（见第8章）。

注：ISO19011：2002《质量和/或环境管理体系审核指南》，也可以为进行内部ISMS审核提供指导。

7 ISMS 管理评审

7.1 总则

管理者应按策划的时间间隔（至少一年一次）评审组织的ISMS，以确保其

持续的适宜性、充分性和有效性。评审应包括评估ISMS改进的机会和变更的需要，包括安全策略和安全目标。评审结果应清楚地写入文件，并保持记录（见4.3.3）。

7.2 评审输入

管理评审的输入应包括：

a) ISMS审计和评审的结果；
b) 相关方的反馈；
c) 组织用于改进ISMS执行和有效性的技术、产品或程序；
d) 纠正和预防措施的实施情况；
e) 上次风险评估未充分指出的脆弱性或威胁；
f) 有效性测量的结果；
g) 上次管理评审所采取措施的跟踪验证；
h) 任何可能影响ISMS的变更；
i) 改进的建议。

7.3 评审输出

管理评审的输出应包括与以下方面有关的任何决定和措施：

a) ISMS有效性的改进；
b) 更新风险评估和风险处置计划；
c) 必要时，修订影响信息安全的程序和控制措施，以反映可能影响ISMS的内外事件，包括以下方面的变化：
    1). 业务要求；
    2). 安全要求；
    3). 影响现有业务要求的业务过程；
    4). 法律法规要求；
    5). 合同责任；
    6). 风险等级和/或风险接受准则。
d) 资源需求；

e) 改进测量控制措施有效性的方式。

8 ISMS 改进

8.1 持续改进

组织应通过应用信息安全策略、安全目标、审核结果、监视事件的分析、纠正预防措施和管理评审（见第7章）持续改进ISMS的有效性。

8.2 纠正措施

组织应采取措施，消除与ISMS要求不符合的原因，以防止再发生。纠正措施文件程序应定义以下方面的要求：

a) 识别不符合；

b) 确定不符合的原因；

c) 评价确保不符合不再发生所需的措施；

d) 确定和实施所需的纠正措施；

e) 记录所采取措施的结果（见4.3.3）；

f) 评审所采取的纠正措施。

8.3 预防措施

组织应采取措施，以消除与ISMS要求潜在不符合的原因，以防止发生。所采取的预防措施应与潜在问题的影响相适宜。预防措施文件程序应规定以下方面的要求：

a) 识别潜在的不符合及其原因；

b) 评估预防不符合发生所需的措施；

c) 确定并实施所需的预防措施；

d) 记录所采取措施的结果（见4.3.3）；

e) 评审所采取的预防措施。

组织应识别发生变化的风险，并通过关注风险的显著变化来识别预防措施要

求。

应根据风险评估结果来确定预防措施的优先级。

注：预防不符合的措施通常比纠正措施更节约成本。

附录 A

控制目标和控制措施

表A.1 中所列出的控制目标与控制措施直接从引用**ISO/IEC17799：2005** 第**5** 到**15** 章。表中列出的控制目标与控制措施并不详尽，组织可考虑增加其他的控制目标与控制方式。应选择表中的控制目标与控制措施作为**4.2.1**

规定的ISMS 过程的一部分**ISO/IEC17799：2005** 第**5** 到**15** 章为支持**A.5** 到**A.15** 规定的控制提供最佳惯例的实施建议和指南。

表A.1 控制目标和控制措施

A.5 安全策略		
A.5.1 信息安全策略 目标：为信息安全提供符合业务要求和相关法律法规的管理指导和支持		
A.5.1.1	信息安全策略文档	*控制措施：* 信息安全策略文档应经过管理层的批准，并向所有员工和外部相关方发布和沟通
A.5.1.2	信息安全策略评审	*控制措施：* 应按计划的时间间隔或当发生重大变化时，对信息安全策略文档进行评审，以确保其持续的适宜性、充分性和有效性
A.6 信息安全组织		
A.6.1 内部组织 目标：在组织内部管理信息安全		
A.6.1.1	信息安全管理承诺	*控制措施：* 管理者应通过清晰的方向、可见的承诺、明确的任务分配、信息安全职责沟通在组织内积极支持安全
A.6.1.2	信息安全协调	*控制措施：* 信息安全活动应由组织各部门及各种相关角色和职能的代表进行协作
A.6.1.3	信息安全职责分配	*控制措施：* 应明确定义所有的信息安全职责
A.6.1.4	信息处理设施授权过程	*控制措施：* 应定义并实施对信息处理设施的管理授权过程
A.6.1.5	保密协议	*控制措施：* 应定义并定期评审组织的保密或非扩散协议。该协议反应组织对于信息保护的要求。

A.6.1.6	与监管机构的联系	*控制措施：* 应保持与相关监管机构的适当联系
A.6.1.7	与特殊利益团体的联系	*控制措施：* 应保持与特殊利益团体或其他专业安全协会和行业协会的适当联系
A.6.1.8	信息安全独立评审	*控制措施：* 应按计划的时间间隔或当发生重大的信息安全变化时，对组织的信息安全管理方法及其实施情况（如，信息安全控制目标、控制措施、策略、过程和程序）进行独立评审
A.6.2 外部组织 目标：保持组织的被外部组织访问、处理、沟通或管理的信息及信息处理设备的安全		
A.6.2.1	识别与外部组织相关的风险	*控制措施：* 应识别来自涉及外部组织的业务过程的信息和信息处理设施的风险，并在允许访问前实施适当的控制
A.6.2.2	当与顾客接触时强调安全	*控制措施：* 应在允许顾客访问组织的信息或资产前强调所有的被定义的安全要求
A.6.2.3	在第三方协议中强调安全	*控制措施：* 与第三方签订的协议中应覆盖所有相关的安全要求。这些协议可能涉及对组织的信息或信息处理设施的访问、处理、沟通或管理，或增加信息处理设施的产品和服务。
A.7 资产管理		
A.7.1 资产责任 目标：实现并保持组织资产的适当保护		
A.7.1.1	资产清单	*控制措施：* 应清楚识别所有的资产，编制并保持所有重要资产清单
A.7.1.2	资产所有权	*控制措施：* 所有信息及与信息处理设施有关的资产应由组织指定的部门负责
A.7.1.3	资产的有效使用	*控制措施：* 应识别信息及与信息处理设施有关的资产的有效使用的使用准则，形成文件并实施
A.7.2 资产分类 目标：确保信息可以得到适当程度的保护		
A.7.2.1	分类指南	控制措施： 应按照信息的价值、法律要求及对组织的敏感程度和关键程度进行分类
A.7.2.2	信息标识和处置	控制措施： 应制定一套与组织所采用的分类方案一致的信息标识和处置的程序，并实施
A.8 人力资源安全		
A.8.1 雇佣前		

目标：确保员工、承包方和第三方用户了解他们的责任并适合于他们所考虑的角色，减少盗窃、滥用或设施误用的风险		
A.8.1.1	角色和职责	*控制措施：* 应根据组织的信息安全策略，定义员工、承包方和第三方用户的安全角色和职责并形成文件
A.8.1.2	筛选	*控制措施：* 应根据相关的法律、法规和道德，对所有的求职者、承包方和第三方用户进行背景验证检查，该检查应与业务要求、被访问信息的类别及已知风险相适宜
A.8.1.3	雇佣条款和条件	*控制措施：* 作为合同责任的一部分，员工、承包方和第三方用户应统一并签署他们的雇佣合同的条款和条件。这些条款和条件应规定他们和组织对于信息安全的责任
A.8.2 雇佣中 目标：确保所有的员工、承包方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全策略，减少人为错误的风险		
A.8.2.1	管理职责	*控制措施：* 管理者应要求所有的员工、承包方和第三方用户应用符合组织已建立的策略和程序的安全
A.8.2.2	信息安全意识、教育和培训	*控制措施：* 组织应对组织的所有员工，适当时，还包括合同方和第三方用户进行适当的意识培训、定期更新的、与他们工作相关的组织策略和程序培训
A.8.2.3	惩戒过程	*控制措施：* 应建立一个正式的员工违反安全的惩戒过程
A.8.3 雇佣终结或变更 目标：确保员工、承包方和第三方用户离开组织或变更雇佣关系时以一种有序的方式进行		
A.8.3.1	终结责任	*控制措施：* 应清晰定义和分配进行雇佣变更或终结的责任
A.8.3.2	归还资产	*控制措施：* 当结束雇佣关系、合同或协议时，员工、承包方和第三方用户应归还所使用的组织资产
A.8.3.3	废除访问权限	*控制措施：* 当雇佣关系、合同或协议终止时，应废除所有员工、承包方和第三方用户对信息和信息处理设施的访问权限，或根据变化调整
A.9 物理与环境安全		
A.9.1 安全区域 目标：防止对组织办公场所和信息的非授权物理访问、破坏和干扰		
A.9.1.1	物理安全边界	*控制措施：* 组织应使用安全边界（障碍物，如墙、控制进入大门的卡或人工接待台）来保护包含信息和信息处理设施的区域
A.9.1.2	物理进入控制	*控制措施：* 应通过适当进入控制对安全区域进行保护，以确保只

		有经过授权的人员才可以访问
A.9.1.3	办公室、场所和设施的安全	*控制措施：* 应设计并实施保护办公室、场所和设施的物理安全
A.9.1.4	防范外部和环境威胁	*控制措施：* 应设计并实施针对火灾、水灾、地震、爆炸、骚乱和其他形式的自然或人为灾难的物理保护措施
A.9.1.5	在安全工作区域	*控制措施：* 应设计并实施在安全区域工作的物理保护和指南
A.9.1.6	公共访问和装卸区域	控制措施： 访问区域如装卸区域，及其他未经授权人员可能进入办公场所的地点应加以控制，如果可能的话，与信息处理设施加以隔离以防止非授权的访问
A.9.2 设备安全 目标：预防资产的丢失、损坏或被盗，以及对组织业务活动的干扰		
A.9.2.1	设备选址和保护	*控制措施：* 应对设备进行选址安置或保护，以减少来自环境的威胁或危害，并减少未授权访问的机会
A.9.2.2	支持设施	*控制措施：* 应保护设备免受电力中断或其他因为支持性设施失效所导致的中断
A.9.2.3	电缆安全	控制措施： 应保护承载数据或支持信息服务的电力和通讯电缆免遭中断或破坏
A.9.2.4	设备维护	*控制措施：* 应正确维护设备，以确保其持续的可用性和完整性
A.9.2.5	场外设备安全	*控制措施：* 应对场外设备进行安全防护，考虑在组织边界之外工作的不同风险
A.9.2.6	设备的安全销毁或重用	*控制措施：* 应检查包含存储介质的设备，以确保在销毁前所有敏感数据或授权软件已经被删除或安全重写
A.9.2.7	财产转移	*控制措施：* 未经授权，不得将设备、信息或软件带离
A.10 通讯及操作管理		
A.10.1 操作程序及职责 目标：确保信息处理设施的正确和安全操作		
A.10.1.1	文件化的操作程序	*控制措施：* 应编制并保持文件化的操作程序，并确保所有需要的用户可以获得
A.10.1.2	变更管理	*控制措施：* 应控制信息处理设施及系统的变更
A.10.1.3	职责分离	控制措施： 应分离职责和责任区域，以降低未授权访问、无意识修改或滥用组织资产的机会
A.10.1.4	开发、测试和运营设	*控制措施：*

	施的分离	应分离开发、测试和运营设施，以降低未授权访问或对操作系统变更的风险
A.10.2 第三方服务交付管理 目标：实施并保持信息安全的适当水平，确保第三方交付的服务符合协议要求		
A.10.2.1	服务交付	*控制措施：* 确保第三方实施、运作并保持第三方服务交付协议中包含的安全控制、服务定义和交付等级
A.10.2.2	第三方服务的监督和评审	*控制措施：* 应对第三方的服务和提交的报告、记录定期进行监视和评审，并定期进行审计
A.10.2.3	第三方服务的变更管理	*控制措施：* 应管理提供服务的变更（包括保持和改进现有信息安全策略、程序和控制措施），考虑对业务系统的关键程度、涉及的过程和风险的再评估
A.10.3 系统规划与验收 目标：最小化系统失效的风险		
A.10.3.1	能力管理	*控制措施：* 应监督、调整资源的使用情况，并反应将来能力的要求，以确保系统的性能
A.10.3.2	系统验收	*控制措施：* 应建立新的信息系统、系统升级和新版本的验收准则，并在开发过程中及接收前进行适当的系统测试
A.10.4 防范恶意代码和移动代码 目标：保护软件和信息的完整性		
A.10.4.1	控制恶意代码	*控制措施：* 应实施防范恶意代码的检测、预防和恢复，以及适当的用户意识程序
A.10.4.2	控制移动代码	*控制措施：* 当使用移动代码获得授权时，配置管理应确保授权的移动代码按照明确定义的安全策略运行，并防止未经授权移动代码的执行
A.10.5 备份 目标：保持信息和信息处理设施的完整性和可用性		
A.10.5.1	信息备份	*控制措施：* 应根据既定的备份策略，对信息和软件进行备份并定期测试
A.10.6 网络安全管理 目标：确保网络中的信息和支持性基础设施得到保护		
A.10.6.1	网络控制	*控制措施：* 应对网络进行充分的管理和控制，以防范威胁、保持使用网络的系统和应用程序的安全，包括传输的信息
A.10.6.2	网络服务的安全	*控制措施：* 应识别所有网络服务的安全特性、服务等级和管理要求，并包含在网络服务协议中，无论这种服务是由内部提供的还是外包的。

A.10.7 介质处置 目标：防止对资产的未授权泄漏、修改、移动或损坏，及对业务活动的干扰		
A.10.7.1	可移动介质的管理	*控制措施：* 应建立可移动介质的管理程序
A.10.7.2	介质销毁	*控制措施：* 当介质不再需要时，应按照正式的程序进行安全可靠的销毁
A.10.7.3	信息处理程序	*控制措施：* 应建立信息处理和存储程序，以防范该信息的未授权泄漏或误用
A.10.7.4	系统文档安全	*控制措施：* 应保护系统文档免，受未授权的访问
A.10.8 信息交换 目标：应保持组织内部或组织与外部组织之间交换信息和软件的安全		
A.10.8.1	信息交换策略和程序	*控制措施：* 应建立正式的交换策略、程序和控制，以保护通过所有类型的通讯设施交换信息的安全
A.10.8.2	交换协议	*控制措施：* 应建立组织和外部组织之间的信息和软件交换的协议
A.10.8.3	物理介质传输	*控制措施：* 在组织的物理边界之外进行传输的过程中，应保护包含信息的介质免受未授权的访问、误用或破坏
A.10.8.4	电子消息	*控制措施：* 应适当保护电子消息的信息
A.10.8.5	业务信息系统	*控制措施：* 应开发并实施策略和程序，以保护与业务信息系统互联的信息
A.10.9 电子商务服务 目标：确保电子商务的安全及他们的安全使用		
A.10.9.1	电子商务	*控制措施：* 应保护电子商务中通过公共网络传输的信息，以防止欺诈、合同争议、未授权的泄漏和修改
A.10.9.2	在线交易	*控制措施：* 应保护在线交易中的信息，以防止不完整的传输、路由错误、未授权的消息修改、未经授权的泄漏、未经授权的消息复制或回复
A.10.9.3	公共可用信息	*控制措施：* 应保护公共可用系统中信息的完整性，以防止未经授权的修改
A.10.10 监督 目标：检测未经授权的信息处理活动		
A.10.10.1	审计日志	*控制措施：* 应产生记录用户活动、意外和信息安全事件的日志，并按照约定的期限进行保留，以支持将来的调查和访问控制监视

A.10.10.2	监视系统的使用	*控制措施：* 应建立监视信息处理系统使用的程序，并定期评审监视活动的结果
A.10.10.3	日志信息保护	*控制措施：* 应保护日志设施和日志信息免受破坏和未授权的访问
A.10.10.4	管理员和操作者日志	*控制措施：* 应记录系统管理员和系统操作者的活动
A.10.10.5	错误日志	控制措施： 应记录并分析错误日志，并采取适当的措施
A.10.10.6	时钟同步	*控制措施：* 组织内或统一安全域内的所有相关信息处理设施的时钟应按照约定的正确时间源保持同步
A.11 访问控制		
A.11.1 访问控制的业务要求 目标：控制信息访问		
A.11.1.1	访问控制策略	*控制措施：* 应建立文件化的访问控制策略，并根据对访问的业务和安全要求进行评审
A.11.2 用户访问管理 目标：确保授权用户的访问，并预防信息系统的非授权访问		
A.11.2.1	用户注册	*控制措施：* 应建立正式的用户注册和解除注册程序，以允许和撤销对于所有信息系统和服务的访问
A.11.2.2	特权管理	*控制措施：* 应限制和控制特权的使用和分配
A.11.2.3	用户口令管理	*控制措施：* 应通过正式的管理流程控制口令的分配
A.11.2.4	用户访问权限的评审	*控制措施：* 管理者应按照策划的时间间隔通过正式的流程对用户的访问权限进行评审
A.11.3 用户责任 目标：预防未授权用户的访问，信息和信息处理设施的破坏或被盗		
A.11.3.1	口令使用	*控制措施：* 应要求用户在选择和使用口令时遵循良好的安全惯例
A.11.3.2	无人值守的用户设备	*控制措施：* 用户应确保无人值守的设备得到适当的保护
A.11.3.3	清除桌面及屏幕策略	*控制措施：* 应采用清楚桌面纸质和可移动存储介质的策略，以及清楚信息处理设施所采用的清除屏幕策略
A.11.4 网络访问控制 目标：防止对网络服务未经授权的访问		
A.11.4.1	网络服务使用策略	*控制措施：* 用户应只能访问经过明确授权使用的服务

A.11.4.2	外部连接用户的鉴别	*控制措施：* 应使用适当的鉴别方法控制远程用户的访问
A.11.4.3	网络设备的识别	*控制措施：* 应考虑将自动设备识别作为鉴别特定区域和设备连接鉴别的方法
A.11.4.4	远程诊断和配置端口保护	*控制措施：* 应控制对诊断和配置端口的物理和逻辑访问
A.11.4.5	网内隔离	*控制措施：* 应隔离网络上的的信息服务组、用户和信息系统
A.11.4.6	网络连接控制	*控制措施：* 在公共网络中，尤其是那些延展到组织边界之外的网络，应限制用户联接的能力，并与业务应用系统的访问控制策略和要求一致（见11.1）
A.11.4.7	网络路由控制	*控制措施：* 应对网络进行路由控制，以确保信息联接和信息流不违反业务应用系统的访问控制策略
A.11.5 操作系统访问控制 目标：防止对操作系统的未授权访问		
A.11.5.1	安全登陆程序	*控制措施：* 应通过安全登陆程序对操作系统的访问进行控制
A.11.5.2	用户标识和鉴别	*控制措施：* 所有的用户应有一个唯一的识别码（用户ID）且仅供本人使用，应使用适当的鉴别技术来证实用户所声称的身份
A.11.5.3	口令管理系统	*控制措施：* 应使用交互式口令管理系统，并确保口令质量
A.11.5.4	系统设施的使用	*控制措施：* 应限制并严格控制设施程序的使用和应用系统控制的使用
A.11.5.5	终端时限	*控制措施：* 在超过规定的不工作状态时限之后，应关闭终端
A.11.5.6	连接时间限制	*控制措施：* 应使用连接时间限制以提供高风险应用程序的额外安全保障
A.11.6 应用系统和信息访问控制 目标：防止对应用系统中信息的未授权访问		
A.11.6.1	信息访问限制	*控制措施：* 应根据规定的访问控制策略，限制用户和支持人员对信息和应用系统功能的访问
A.11.6.2	敏感系统隔离	*控制措施：* 敏感系统应使用隔离的计算环境
A.11.7 移动计算和远程工作 目标：确保在使用移动计算和远程工作设施时信息的安全		
A.11.7.1	移动计算和通讯	*控制措施：* 应建立正式的策略并实施适当的措施，以防范使用移动计算和通讯设施的风险

A.11.7.2	远程工作	*控制措施：* 应开发并实施远程工作的策略、操作计划和程序
A.12 信息系统的获取、开发和维护		
A.12.1 信息系统安全要求 目标：确保安全成为信息系统的内置部分		
A.12.1.1	安全要求分析和规范	*控制措施：* 新的信息系统或对现有信息系统的更新的业务要求声明中应规定安全控制的要求
A.12.2 应用系统的正确处理 目标：防止应用系统信息的错误、丢失、未授权的修改或误用		
A.12.2.1	输入数据确认	*控制措施：* 应验证应用系统输入数据，以确保正确和适当
A.12.2.2	内部处理控制	*控制措施：* 应用系统中应包含确认检查，以检测数据处理过程中的错误
A.12.2.3	消息完整性	*控制措施：* 应识别应用系统中确保鉴别和保护消息完整性的要求，识别并实施适当的控制
A.12.2.4	输出数据确认	*控制措施：* 应确认应用系统输出的数据，以确保存储的信息的处理是正确的并与环境相适宜
A.12.3 加密控制 目标：通过加密手段来保护细腻的保密性、真实性或完整性		
A.12.3.1	使用加密控制的策略	*控制措施：* 为保护信息，应开发并实施加密控制的使用策略
A.12.3.2	密钥管理	*控制措施：* 应进行密钥管理，以支持组织对密码技术的使用
A.12.4 系统文档安全 目标：确保系统文档的安全		
A.12.4.1	操作软件控制	*控制措施：* 应建立程序，对操作系统软件安装进行控制
A.12.4.2	系统测试数据的保护	*控制措施：* 应谨慎选择测试数据，并加以保护和控制
A.12.4.3	源代码库的访问控制	*控制措施：* 应限制对源代码库的访问
A.12.5 开发和支持过程的安全 目标：保持应用系统软件和信息的安全		
A.12.5.1	变更控制程序	*控制措施：* 应通过正式的变更控制程序，控制变更的实施
A.12.5.2	操作系统变更后的技术评审	*控制措施：* 当操作系统变更后，应评审并测试关键的业务应用系统，以确保变更不会对组织的运营或安全产生负面影响
A.12.5.3	软件包变更限制	*控制措施：* 不鼓励对软件包进行变更。对必要的更改严格控制

A.12.5.4	信息泄漏	*控制措施：* 防止信息泄漏的机会
A.12.5.5	软件外包开发	控制措施： 组织应对软件外包开发进行监控
A.12.6 技术漏洞管理 目标：减少由利用公开的技术漏洞带来的风险		
A.12.6.1	控制技术漏洞	*控制措施：* 应及时获得组织所使用的信息系统的技术漏洞的信息，评估组织对此类技术漏洞的保护，并采取适当的措施
A.13 信息安全事故管理		
A.13.1 报告信息安全事件和弱点 目标：确保与信息系统有关的安全事件和弱点的沟通能够及时采取纠正措施		
A.13.1.1	信息安全事件报告	*控制措施：* 应通过适当的管理途径尽快报告信息安全事件
A.13.1.2	报告信息安全弱点	*控制措施：* 应要求所有的员工、承包方和第三方用户注意并报告系统或服务中已发现或疑似的安全弱点
A.13.2 信息安全事故的管理和改进 目标：确保使用持续有效的方法管理信息安全事故		
A.13.2.1	职责和程序	*控制措施：* 应建立管理职责和程序，以快速、有效和有序的响应信息安全事故
A.13.2.2	从信息安全事故中学习	*控制措施：* 应建立能够量化和监控信息安全事故的类型、数量、成本的机制
A.13.2.3	收集证据	*控制措施：* 事故发生后，应根据相关法律的规定（无论是民法还是刑法）跟踪个人或组织的行动，应收集、保留证据，并以符合法律规定的形式提交
A.14 业务连续性管理		
A.14.1 业务连续性管理的信息安全方面 目标:防止业务活动的中断,保护关键业务流程不会受信息系统重大失效或自然灾害的影响,并确保他们的及时恢复		
A.14.1.1	在业务连续性管理过程中包含信息安全	*控制措施：* 应在组织内开发并保持业务连续性管理过程，该过程阐明了组织的业务连续性对信息安全的要求
A.14.1.2	业务连续性和风险评估	*控制措施：* 应识别可能导致业务过程中断的事故，以及这类中断发生的可能性和影响、中断的信息安全后果
A.14.1.3	开发并实施包括信息安全的连续性计划	*控制措施：* 应开发并实施计划，以确保在关键业务流程中断或失效后能够在要求的时间内和要求的等级上保持和恢复运营并确保信息的可用性
A.14.1.4	业务连续性计划框架	控制措施：

		应保持一个单独的业务连续性计划框架，以确保所有计划的一致性，以维护信息安全要求的一致性并识别测试和保持的优先级
A.14.1.5	BCP 的测试、保持和再评估	*控制措施：* 应定期测试并更新BCP，以确保BCP 的更新和有效
A.15 符合性		
A.15.1 与法律法规要求的符合性 目标：避免违反法律、法规、规章、合同要求和其他的安全要求		
A.15.1.1	识别使用的法律法规	*控制措施：* 应清晰规定所有相关的法律、法规和合同要求以及组织满足这些要求的方法并形成文件，并针对每个信息系统和组织进行更新
A.15.1.2	知识产权（IPR）	*控制措施：* 应实施适当的程序，以确保在使用与知识产权有关的材料和软件时符合法律法规和合同要求
A.15.1.3	组织记录的保护	*控制措施：* 应按照法律法规、合同和业务要求，保护重要记录免受损失、破坏或伪造篡改
A.15.1.4	数据保护和个人信息的隐私	*控制措施：* 应确保按适用的法律法规，适用时，还有合同条款的要求来保护数据和隐私
A.15.1.5	防止信息处理设施的误用	*控制措施：* 应阻止用户把信息处理设施用于非授权的目的
A.15.1.6	加密控制法规	*控制措施：* 使用密码控制时，应确保遵守相关的协议、法律法规
A.15.2 符合安全策略、标准，技术符合性 目标：确保系统符合组织安全策略和标准		
A.15.2.1	符合安全策略和标准	*控制措施：* 管理者应确保在其职责范围内的所有安全程序得到了正确实施，以符合安全策略和目标
A.15.2.2	技术符合性检查	*控制措施：* 应定期检查信息系统与安全实施标准的符合程度
A.15.3 信息系统审计的考虑因素 目标：最大化信息系统审计的有效性，最小化来自/对信息系统审计的影响		
A.15.3.1	信息系统审计控制	*控制措施：* 应谨慎规划对操作系统检查所涉及的审计要求和活动并获得许可，以最小化对业务过程中断的风险
A.15.3.2	信息系统审核工具保护	*控制措施：* 应限制对信息系统审计工具的访问，以防止可能的误用或损坏

附录 B

OECD 准则和本国际标准

OECD 指导所提供的信息系统及网络安全准则应用于信息系统及网络安全的所有策略和操作标准。本标准为实施 OECD 准则部分内容提供一个信息安全管理体系框架，该框架运用 PDCA 模型及在第 4, 5, 6 和 8 章中所描述的过程，在表 B.1 中简要说明.

表 B.1-OECD 准则与 PDCA 模型

OECD 准则	对应的 ISMS 过程和 PDCA 阶段
意识 参与者应该意识到信息体系和网络的安全需要以及他们为增强安全所能做的工作。	该活动为 **DO** 阶段的部分（见 4.2.2 和 5.2.2）
责任 所有的参与者对信息体系和网络的安全负责	该活动为 **DO** 阶段的部分（见 4.2.2 和 5.1）
响应 参与者应该采取及时、协作的行动，对安全事件进行预防、检测、响应。	这部分为 **Check** 阶段的监视活动（见 4.2.3 和 6 到 7.3）和 **Act** 阶段响应活动（见 4.2.4 和 8.1 到 8.3）。 这部分也被 **Plan** 和 **Check** 阶段的部分内容所覆盖。
风险评估 参与者应该进行风险评估	该活动是 **Plan** 阶段的部分（见 4.2.1），风险评估为 **Check** 阶段的部分（见 4.2.3 和 6 到 7.3）
安全设计与实施 参与者应该使安全成为信息体系和网络的基本的组成部分	如果风险评估被实施，作为 **Plan** 阶段的一部分，控制措施将被用来风险处置（见 4.2.1）。**Do** 阶段将覆盖这些控制措施的实施和操作使用（见 4.2.2 和 5.2）。
安全管理 参与者应该采取综合处理方法来进行安全管理	风险管理是一个过程，该过程包括预防、事件检测与响应、进行中的持续、评审和审计。所有的这些方面在 **Plan**、**Do**、**Check** 和 **Act** 阶段包含。
再评估 参与方应评审、再评估信息系统与网络的安全，并对策略、事件、方法和程序进行适当的修改。	信息安全再评估为 **Check** 阶段（见 4.1.3 和 6 到 7.3）的部分，在这个阶段中，应该进行定期的评审来检查信息安全管理系统的有效性。改进信息安全（见 4.2.4 和 8.1 到 8.3）。

附录 C

ISO9001:2000, ISO14001:2004 与本标准对应关系

表 C.1 说明了 ISO9001:2000，ISO14001:2004 与本标准的对应关系。

表 C.1-ISO9001:2000，ISO14001:2004 与本标准的对应关系

本校准	ISO 9001:2000	ISO14001:2004
简介 总则 过程方法 与其他管理体系的兼容性	**简介** 总则 过程方法 与 ISO 9004 的关系 与其他管理体系的兼容性	**简介**
1 范围 1.1 总则 1.2 应用	**1 范围** 1.1 总则 1.2 应用	**1 范围**
2 引用标准	**2 引用标准**	**2 引用标准**
3 术语和定义	**3 术语和定义**	**3 术语和定义**
4 信息安全管理体系 4.1 总体要求 4.2 建立并管理 ISMS 4.2.1 建立 ISMS 4.2.2 实施和运作 ISMS 4.2.3 监视和评审 ISMS	**4 质量管理体系** 4.1 总体要求 8.2.3 过程的监视和测量 8.2.4 产品的监视和测量	**4 EMS 要求** 4.1 总体要求 4.4 实施和运作 4.5.1 监视和测量

本校准	ISO 9001:2000	ISO14001:2004
4.2.4 保持和改进 ISMS		
4.3 文件要求 4.3.1 总则 4.3.2 文件控制 4.3.3 记录控制	4.2 文件要求 4.2.1 总则 4.2.2 质量手册 4.2.3 文件控制 4.2.4 记录控制	 4.4.5 文件控制 4.5.4 记录控制
5 管理职责 5.1 管理承诺	**5 管理职责** 5.1 管理承诺 5.2 以顾客为关注焦点 5.3 质量策略 5.4 策划 5.5 职责、权限和沟通	 4.2 环境策略 4.3 策划
5.2 资源管理 5.2.1 资源提供 5.2.2 意识培训和能力	**6 资源管理** 6.1 资源的提供 6.2 人力资源 6.2.2 能力、意识和培训 6.3 基础设施 6.4 工作环境	 4.4.2 能力、意识和培训
6 ISMS 内部审计	8.2.2 内部审计	4.5.5 内部审计
7 ISMS 管理评审 7.1 总则 7.2 评审输入 7.3 评审输出	**5.6 管理评审** 5.6.1 总则 5.6.2 评审输入 5.6.3 评审输出	**4.6 管理评审**
8 ISMS 改进 8.1 持续改进	**8.5 改进** 8.5.2 持续改进	

本校准	ISO 9001:2000	ISO14001:2004
8.2 纠正措施	8.5.2 纠正措施	4.5.3 不符和，纠正措施和保护措施
8.3 预防措施	8.5.3 预防措施	
附录 A 控制目标和控制措施 **附录 B OECD 准则和本国际标准** **附录 C ISO9001:2000，ISO14001:2004 与本标准的对应关系**		**附录 A 本标准使用指南** **附录B 与ISO14001:2004 and ISO 9001:2000**

参考资料

Standards publications

[1] ISO 9001:2000, Quality management systems — Requirements.

[2] ISO/IEC 13335-1:2004, Management of information and communications technology security — Part1: Concepts and models for managing and planning ICT security.

[3] ISO/IEC TR 13335-3:1998, Guidelines for the Management of IT Security — Part 3: Techniques for the management of IT security.

[4] ISO/IEC TR 13335-4:2000, Guidelines for the Management of IT Security — Part 4: Selection of safeguards.

[5] ISO 14001:2004, Environmental management systems — Requirements with guidance for use.

[6] ISO/IEC TR 18044:2004, Security techniques — Information Security Incident Management.

[7] SO 19011:2002, Guidelines for quality and/or environmental management systems auditing.

[8] ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems.

[9] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards.

Other publications

[1] OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[2] NIST SP 800-30, Risk Management Guide for Information Technology Systems.

[3] Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study,1986.